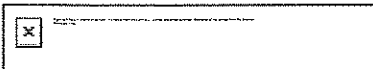


12802

Asci, Terry (SCA)

From: noreply@formstack.com
Sent: Monday, April 16, 2018 1:00 PM
To: Breaches, Data (SCA)
Subject: Security Breach Notifications



Formstack Submission For: Security Breach Notifications

Submitted at 04/16/18 12:59 PM

Business Name: Golter Law Office

Business Address:

Foreign Business Address:

Company Type: Other

Your Name: Dominic Paluzzi

Title: Member

Contact Address: McDonald Hopkins PLC
38533 Woodward Avenue, Suite 318
Bloomfield Hills, MI 48304

Foreign Contact Address:

Telephone Number: (248) 220-1356

Extension:

Email Address: dpaluzzi@mcdonaldhopkins.com

Relationship to Org: Other

2

Breach Type:	Electronic
Date Breach was Discovered:	03/15/2018
Number of Massachusetts Residents Affected:	1
Person responsible for data breach.:	Unknown
Please give a detailed explanation of how the data breach occurred.:	On October 31, 2017, Golter Law Office learned that a hard drive had been stolen from a Golter employee's vehicle. The crime occurred sometime during that morning or the previous evening. Golter Law Office concluded that the stolen hard drive contained documents and files related to Golter Law Office clients. Since completing the investigation and manual document review of the documents located on the stolen hard drive, on March 15, 2018, Golter Law Office discovered that personal information was contained on the drive. The information that was accessible in the hard drive included name and Social Security number, and may have also included driver's license number, bank account number and/or credit card number.
Please select the type of personal information that was included in the breached data.:	Financial Account Numbers = Selection(s) Social Security Numbers = Selection(s) Driver's License = Selection(s) Credit/Debit Card Number = Selection(s)
Please check ALL of the boxes that apply to your breach.:	The breach was a result of a malicious/criminal act. = Selection(s)
For breaches involving paper: A lock or security mechanism was used to physically protect the data.:	N/A
Physical access to systems containing personal information was restricted to authorized personnel only.:	N/A
Network configuration of breached system:	N/A

For breaches involving electronic systems, complete the following:

N/A = Selection(s)

All Massachusetts residents affected by the breach have been notified of the breach.:

Yes

Method(s) used to notify Massachusetts residents affected by the breach (check all that apply)::

US Mail = Selection(s)

Date notices were first sent to Massachusetts residents (MM/DD/YYYY):

04/13/2018

All Massachusetts residents affected by the breach have been offered complimentary credit monitoring services.:

Yes

Law enforcement has been notified of this data breach.:

Yes

Please describe how your company responded to the breach. Include what changes were made or may be made to prevent another similar breach from occurring.:

Golter Law Office is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Golter Law Office continually evaluates and modifies its practices and internal controls to enhance the security and privacy of personal information.

Asci, Terry (SCA)

From: Czuprynski, Christine <cczuprynski@mcdonaldhopkins.com>
Sent: Monday, April 16, 2018 2:15 PM
To: Breaches, Data (SCA)
Subject: Security Incident Notification
Attachments: Golter Law Office -- Notification to Massachusetts (7342947x7AB84).pdf; Golter law Office - Notice Letter MA (7341134x7AB84).pdf

To Whom it May Concern,

Attached please find a security incident notification filed on behalf of Golter Law Office with the Massachusetts Department of Consumer and Business Affairs this afternoon. Also attached please find the template notice letter used to provide written notice to impacted individuals.

Please let us know if you have questions or would like to discuss.

Thanks,
Chris

Christine Czuprynski
Counsel

T: 248.220.1360
cczuprynski@mcdonaldhopkins.com
www.mcdonaldhopkins.com

39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304

McDonald Hopkins

A business advisory and advocacy law firm®



Mass.gov

Data Breach Notification Submission

Data Breach Notification Submission

Instructions: Please complete the form below to submit a data breach notification to the Office of Consumer Affairs and Business Regulation. You can also print this submission for your own records. Please note under M.G.L. C93H, a separate notification must be sent to the Attorney General's Office.

If you're mailing your submission, please send to: Office of Consumer Affairs and Business Regulation, 501 Boylston St., Suite 5100, Boston, MA 02116

- Individual breaches affecting multiple debit/credit card holders of your organization can be reported on a monthly basis.
- Please do not include any personally identifiable information for Massachusetts residents in any of the fields.

Section I: Organization & Contact Information

Business Name *

Golter Law Office

Business Address (optional)

City

State

ZIP Code

Foreign Business Address (optional)

If your business is located outside the United States, enter the address here

Company Type *

Your Name *

First Name

Last Name

Title *

Member

Contact Address (optional)

McDonald Hopkins PLC

38533 Woodward Avenue, Suite 318

Bloomfield Hills

City

Michigan



State

48304

ZIP Code

Foreign Contact Address (optional)

If your contact address is outside the United States, enter the address here

Telephone Number *

(248) 220-1356

Extension (optional)

Email Address *

Relationship to Org *



Section II: Breach Information

Breach Type *



Date Breach was Discovered *



Number of Massachusetts Residents Affected *

Person responsible for data breach. *



Please give a detailed explanation of how the data breach occurred. *

On October 31, 2017, Golter Law Office learned that a hard drive had been stolen from a Golter employee's vehicle. The crime occurred sometime during that morning or the previous evening. Golter Law Office concluded that the stolen hard drive contained documents and files related to Golter Law Office clients. Since completing the investigation and manual document review of the documents located on the stolen hard drive, on March 15, 2018, Golter Law Office discovered that personal information was contained on the drive. The information that was accessible in the hard drive included name and Social Security number, and may have also included driver's license number, bank account number and/or credit card number.

Please select the type of personal information that was included in the breached data. *

	Selection(s)
Financial Account Numbers	<input checked="" type="checkbox"/>
Social Security Numbers	<input checked="" type="checkbox"/>
Driver's License	<input checked="" type="checkbox"/>
Credit/Debit Card Number	<input checked="" type="checkbox"/>

Please check ALL of the boxes that apply to your breach. *

	Selection(s)
The person(s) with possession of personal information had authorized access	<input type="checkbox"/>
The breach was a result of a malicious/criminal act.	<input checked="" type="checkbox"/>
The breach occurred while the data was being transported outside of your premises.	<input type="checkbox"/>
The breach occurred at the location of a third party service provider.	<input type="checkbox"/>

There is a written contract in place with the third-party provider requiring protection of personal information.

☐

Section III: Security Environment

For breaches involving paper: A lock or security mechanism was used to physically protect the data. *

☐ Yes

☐ No

☒ N/A

Physical access to systems containing personal information was restricted to authorized personnel only. *

☐ Yes

☐ No

☒ N/A

Network configuration of breached system *

N/A



For breaches involving electronic systems, complete the following *

	Selection(s)
Breached data was encrypted.	<input type="checkbox"/>
The key to encrypted data was stolen.	<input type="checkbox"/>

Personal information stored on the breached system was password-protected and/or restricted by user permissions.	<input type="checkbox"/>
N/A	<input checked="" type="checkbox"/>

Section IV: Remediation

All Massachusetts residents affected by the breach have been notified of the breach. *

☒ Yes

☐ No

Method(s) used to notify Massachusetts residents affected by the breach (check all that apply): *

	Selection(s)
E-mail	<input type="checkbox"/>
US Mail	<input checked="" type="checkbox"/>
Online posting	<input type="checkbox"/>
TV/Radio publication	<input type="checkbox"/>
Other	<input type="checkbox"/>

* Date notices were first sent to Massachusetts residents (MM/DD/YYYY) *

04 <input type="button" value="v"/>	13 <input type="button" value="v"/>	2018 <input type="button" value="v"/>	
-------------------------------------	-------------------------------------	---------------------------------------	---

All Massachusetts residents affected by the breach have been offered complimentary credit monitoring services . *

☒ Yes

☐ No

Law enforcement has been notified of this data breach. *

☒ Yes

☐ No

Please describe how your company responded to the breach. Include what changes were made or may be made to prevent another similar breach from occurring. *

Golter Law Office is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Golter Law Office continually evaluates and modifies its practices and internal controls to enhance the security and privacy of personal information.

- Any documents pertaining to the data breach including the letter being sent to the Massachusetts residents must be sent via email to data.breaches@state.ma.us
- Please do not include any personally identifiable information for Massachusetts residents in any email attachment.
- Individual breaches affecting multiple debit/credit card holders of your organization can be reported on a monthly basis.
- Please review the information you have entered and click on the "Submit Form" button below.

SUBMIT FORM

GOLTER LAW OFFICE, LLC
ATTORNEYS AT LAW
Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

**IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY**

<<Date>>

Dear <<Name 1>>:

I am writing with important information regarding a recent security incident. The privacy and security of the personal information belonging to our clients is of the utmost importance to Golter Law Office, LLC ("Golter"). As such, we wanted to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your information.

On October 31, 2017, we learned of a potential security issue. Upon learning of the issue, we promptly notified law enforcement and commenced a thorough investigation. As part of our investigation, we worked very closely with external cybersecurity professionals experienced with addressing these types of incidents.

Since completing our investigation, on March 15, 2018, we concluded that unknown individual(s) may have had access to personal information belonging to our clients. The information that was available included your name and Social Security number. We have no evidence that any of the information has been misused. Nevertheless, out of an abundance of caution, we want to make you aware of the incident.

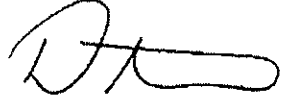
To protect you from potential misuse of your information, we are offering a complimentary one-year membership of Experian IdentityWorksSM Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. IdentityWorks Credit 3B is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft prevention and IdentityWorks Credit 3B, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.

This letter also provides other precautionary measures you can take to protect your personal information, including placing a Fraud Alert, placing a Security Freeze, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

Please accept our apologies that this incident occurred. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at 888-289-2041. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to help protect against potential misuse of your information. The response line is available Monday through Friday, 6:00 a.m. to 6:00 p.m. Pacific Time.

Sincerely,

A handwritten signature in black ink, appearing to read 'D. Golter', with a stylized flourish at the end.

Golter Law Office, LLC
By: David A. Golter

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary 12-Month Credit Monitoring.

To help protect your identity, we are offering a **complimentary** one-year membership of Experian IdentityWorksSM Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: <<Enrollment Deadline>> (Your code will not work after this date.)
2. VISIT the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
PROVIDE the Activation Code: <<Enrollment Code>>

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-288-8057. Be prepared to provide engagement number <<Engagement Number>> as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance^{**}:** Provides coverage for certain costs and unauthorized electronic fund transfers.

**Activate your membership today at <https://www.experianidworks.com/3bcredit>
or call 877-288-8057 to register with the activation code above.**

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-288-8057.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

2. Placing a Fraud Alert.

Whether or not you choose to use the complimentary 12 month credit monitoring services, we recommend that you place an initial 90-day "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax

P.O. Box 105069
Atlanta, GA 30348
www.equifax.com
1-800-525-6285

Experian

P.O. Box 2002
Allen, TX 75013
www.experian.com
1-888-397-3742

TransUnion LLC

P.O. Box 2000
Chester, PA 19016
www.transunion.com
1-800-680-7289

3. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by sending a request in writing, by mail, to all three nationwide credit reporting companies. To find out more on how to place a security freeze on your credit file, you can use the following contact information:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348
<https://www.freeze.equifax.com>
1-800-685-1111

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
<http://experian.com/freeze>
1-888-397-3742

TransUnion Security Freeze

P.O. Box 2000
Chester, PA 19016
<http://www.transunion.com/securityfreeze>
1-888-909-8872

Massachusetts law allows consumers to place a security freeze on their credit reports. If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit reporting agency may charge you up to \$5.00 each to place, temporarily lift, or permanently remove a security freeze. To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies: Equifax, Experian, and TransUnion by regular, certified, or overnight mail at the addresses above.

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, payment by check, money order, or credit card (Visa, MasterCard, American Express, or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit reporting agencies must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both, that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

A credit reporting agency may charge up to \$5.00 to place, lift or remove a security freeze.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

6. Massachusetts Right to Police Report

Under Massachusetts law, you have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.